ГРИНАТОМ
РОСАТОМ

АКЦИОНЕРНОЕ ОБЩЕСТВО «ГРИНАТОМ»
(АО «Гринатом»)

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ СИСТЕМЫ «СИСТЕМА ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ДОСТУПОМ ПОЛЬЗОВАТЕЛЕЙ»

Москва
2024

20.06.2024 22/712-РДП

СОДЕРЖАНИЕ

1 Перечень сокращений, терминов и определений

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированное рабочее место (АРМ) – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида.

Администратор информационной безопасности (АИБ) – лицо, уполномоченное выполнять действия по администрированию (управлению) системой в соответствии с установленной ролью.

Администратор информационной системы (Администратор ИС) – лицо, уполномоченное выполнять действия по администрированию (управлению), обеспечению работы информационной системы в соответствии с установленной ролью.

Администратор АРИДА – лицо, уполномоченное выполнять действия по администрированию (управлению), обеспечению работы программного средства «Система централизованного управления доступом пользователей» в соответствии с установленной ролью.

Ассистент Ролей и Идентификации ДоступА (АРИДА) – в контексте настоящего документа, программное средство «Система централизованного управления доступом пользователей».

Безопасность информации – состояние защищённости информации, при котором обеспечивается её конфиденциальность, доступность и целостность.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы автоматизированной системы.

Госкорпорация «Росатом» - Государственная корпорация по атомной энергии «Росатом».

Доступ к информации – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность – состояние информации, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Информационная безопасность (ИБ) – сохранение конфиденциальности, целостности и доступности информации.

Информационные ресурсы – используемые в информационных системах Госкорпорации «Росатом», АО «Гринатом» (филиалах и обособленном подразделении АО «Гринатом») документы, файлы и базы данных, распоряжение доступом, к которым осуществляется их обладателем путем установления соответствующих правил.

Информационная система (ИС) – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии (ИТ) – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация – сведения (сообщения, данные), независимо от формы их представления.

Информация ограниченного доступа – информация, доступ к которой ограничен на основании законодательства Российской Федерации, отраслевым нормативным документами Госкорпорации «Росатом» и локальным актам АО «Гринатом».

Инцидент информационной безопасности – одно или несколько нежелательных, или неожиданных событий информационной безопасности, которые со значительной степенью вероятности приводят к компрометации операций бизнеса и создают угрозы для информационной безопасности.

Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации, отраслевыми нормативными документами по Госкорпорации «Росатом» и локальными актами АО «Гринатом».

Программное обеспечение (ПО) – совокупность компьютерных программ и программных документов, необходимых для эксплуатации этих программ.

Регламентные работы (РР) – обслуживание технических средств и программного обеспечения, имеющее планово профилактический характер с целью сохранения их эксплуатационных качеств.

Служебная информация ограниченного распространения - несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой, диктуются служебной необходимостью.

Событие безопасности – выявленное состояние системы, услуги или состояния сети, указывающее на возможное нарушение политики обеспечения информационной безопасности, нарушение или отказ мер и средств контроля и управления или прежде неизвестная ситуация, которая может иметь значение для безопасности.

Средство защиты информации (СрЗИ) – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

СЦУДП – Система централизованного управления доступом.

Целостность – свойство сохранения правильности и полноты информации.

DRP – план аварийного восстановления**.**

2 Общие положения

Настоящая Инструкция администратора информационной системы «Система централизованного управления пользователей» (далее – Инструкция) определяет

порядок действий администратора ИС, направленных на обеспечение работоспособности ИС СЦУДП.

Настоящая Инструкция описывает функции и порядок работы администратора ИС СЦУДП (далее – ИС).

Целью разработки Инструкции является определение:

должностных обязанностей администратора ИС;

обязанностей администратора ИС;

прав администратора ИС;

порядка установки компонентов ИС;

порядка изменений условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

порядка осуществления контроля функционирования ИС.

Инструкция предназначена для ознакомления и использования в работе администраторами ИС.

К администраторам ИС также относится администратор АРИДА, выполняющий обязанности в рамках своих компетенций, направленных на обеспечение работоспособности ИС в части АРИДА.

Администратор ИС должен руководствоваться в своей деятельности:

нормативными правовыми актами, методическими документами и национальными стандартами Российской Федерации в области защиты информации;

локально-нормативными актами, распорядительными документами, приказами, распоряжениями Госкорпорации «Росатом», акционерного общества (далее - АО) «Гринатом» и указаниями вышестоящего руководства;

эксплуатационной документацией на компоненты ИС;

руководством администратора ИС;

настоящей и должностной инструкциями.

Администратор ИС должен обладать следующими знаниями:

отраслевая и корпоративная нормативно-методическая документация;

порядок взаимодействия со смежными подразделениями, обеспечивающими безопасное функционирование СЦУДП и предоставляющими услуги в части ИБ.

Администратор ИС должен обладать следующими знаниями и навыками:

установка и настройка компонентов ИС и дополнительных программ, необходимых для корректной и безопасной работы ИС;

необходимых эксплуатационных документов для успешного администрирования ИС;

администрирование ИС;

уверенная работа со специализированным и офисным ПО.

Основной администратор ИС назначается распорядительным документом АО «Гринатом».

На период длительного отсутствия (отпуска, болезни, командировки) основного администратора ИС должен назначаться временно исполняющий обязанности администратора ИС работник, обладающий навыками работы администратора – резервный администратор ИС.

Администратор ИС должен быть ознакомлен под подпись с настоящей инструкцией. Лист ознакомления приведён в приложении к настоящей Инструкции.

3 Основные задачи и функции администратора информационной системы

Основными задачами администратора ИС, выполняющего работы по обеспечению работы ИС, являются:

установка и настройка программного обеспечения, необходимого для безотказной работы ИС и с привлечением, при необходимости, ответственных в рамках услуг;

обслуживание операционных систем, баз данных ИС, системного и прикладного ПО в рамках своей компетенции и с привлечением, при необходимости, ответственных в рамках услуг;

сопровождение системных и прикладных программных средств, функционирующих в ИС, на этапе их жизненного цикла и при выводе их из эксплуатации;

мониторинг, обнаружение и устранение сбоев в работе ИС с привлечением, при необходимости, ответственных в рамках услуг;

резервное копирование и восстановление данных ИС с привлечением, при необходимости, ответственных в рамках подключенных услуг;

поддержка пользователей и решение технических проблем;

участие в закупочных процедурах для нужд ИС в части формирования требований.

Для выполнения поставленных задач на администратора ИС возлагаются следующие функции:

администрирование и сопровождение ИС на этапах ее жизненного цикла и при выводе из эксплуатации;

разработка документов (проектное решение, техническое решение и др.), требуемых для функционирования ИС и реализации интеграции других ИС с ИС СЦУДП;

взаимодействие с администраторами СрЗИ и ИБ, в части обновления версий СрЗИ, системных и прикладных программных средств, установленных в ИС;

участие в проводимых на специализированных площадках мероприятиях, посвященных ИБ;

подготовка предложений по развитию и обучению сотрудников, выполняющих функции администраторов ИС.

4 Функциональные и должностные обязанности администратора информационной системы

Функциональные обязанности администратора ИС:

уведомлять непосредственного руководителя о намерении убытия за пределы Российской Федерации;

знание состава, порядка эксплуатации и перечня решаемых задач эксплуатируемых средств и механизмов обработки информации в ИС;

контроль обеспечения бесперебойного функционирования программных средств в ИС;

анализ содержимого журналов системных событий и log-файлов программного обеспечения, функционирующего в ИС;

обеспечение своевременного архивирования журналов событий и обеспечение надлежащего режима их хранения с установленной периодичностью;

восстановление работоспособности СрЗИ СЦУДП (АРИДА) совместно с АИБ и механизмов защиты информации при выходе их из строя вследствие нештатных (аварийных) ситуаций или устранения последствий стихийного или техногенного характера;

участие в проведении расследований инцидентов информационной безопасности ИС в случае привлечения его АИБ, а также, предотвращении аналогичных инцидентов ИБ в будущем;

участие в анализе материалов событий безопасности ИС в случае его привлечения АИБ;

осуществление непосредственного контроля за внесением изменений в конфигурацию (модификацию) программных, программно-аппаратных средств, установкой и настройкой ПО, функционирующего в ИС;

участие в разработке, согласовании и внесении изменений в нормативную документацию, регламентирующую правила и требования по работе в ИС;

соблюдение общепринятых правил деловой этики и норм общения, а также рамок законодательства Российской Федерации и отраслевой, нормативной и методической документации Госкорпорации «Росатом» и АО «Гринатом»;

доведение до непосредственного руководителя информации обо всех выявленных недостатках и несоответствиях в пределах своей компетенции.

В обязанности администратора ИС также входит:

организация, координация и контроль выполнения мероприятий по установке компонент ИС;

осуществление консультаций пользователей по корректной работе в ИС;

администрирование конфигурации ИС с извещением АИБ СЦУДП;

настройка необходимых прав для пользователей ИС по согласованию с АИБ СЦУДП;

обеспечение высокой доступности сервисов ИС.

Дополнительно на администратора АРИДА возлагаются обязанности по согласованию планируемых им действий, связанных с работоспособностью АРИДА, с основным и/или резервным администратором ИС, а в случаях, затрагивающих меры по защите информации, еще и с администратором ИБ.

5 Права администратора информационной системы

Администратор ИС имеет право:

требовать от пользователей и других администраторов ИС предоставления информации в пределах своей компетенции;

вносить на рассмотрение непосредственному руководителю предложения по улучшению и усовершенствованию деятельности и существующих технических решений в пределах своей компетенции;

по согласованию с руководством принимать участие в мероприятиях, способствующих повышению квалификации по профилю своей деятельности;

требовать от пользователей СЦУДП соблюдения установленной технологии обработки информации и выполнения руководств, инструкций и положений по по работе в ИС;

согласовывать самостоятельные решения в области деятельности предусмотренной настоящей Инструкцией;

по согласованию с руководством, принимать участие в мероприятиях, способствующих повышению квалификации по профилю своей деятельности;

взаимодействовать с органами государственной власти, надзорными органами, контрагентами в рамках своей компетенции.

6 Ответственность администратора информационной системы

Администратор ИС несёт предусмотренную законодательством Российской Федерации ответственность за:

ненадлежащее сопровождение ИС в процессе его жизненного цикла;

нарушение правил эксплуатации СрЗИ, либо правил доступа в ИС;

ненадлежащее выполнение своих должностных или функциональных обязанностей;

несвоевременное и неполное выполнение указаний и распоряжений непосредственного руководителя и функционального руководителя, а также приказов и распоряжений вышестоящего руководства;

полноту и достоверность данных, собранных в ходе выполнения возложенных на него настоящей Инструкцией обязанностей и предоставленных руководству;

качество проводимых работ в соответствии с функциональными обязанностями;

разглашение сведений, составляющих информацию ограниченного доступа, в том числе о применяемых системах, методах и способах защиты информации СЦУДП;

разглашение ключевой, аутентификационной и идентификационной информации администраторов и пользователей;

создание, распространение и (или) использование компьютерных программ либо иной информации, заведомо предназначенных для неправомерного воздействия на объекты информатизации Госкорпорации «Росатом», в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в них;

соблюдение требований законодательства Российской Федерации и требований локальных нормативных актов Госкорпорации «Росатом» и нормативной и методической документации АО «Гринатом», эксплуатационной документации на СрЗИ, сертифицированное системное и прикладное программное обеспечение.

Администратору ИС **запрещается**:

используя служебное положение, создавать ложные информационные сообщения и учетные записи пользователей, получать доступ к информации и

предоставлять его другим (третьим) лицам с целью ее распространения, модификации, копирования, уничтожения;

нарушать правила хранения ключевой, аутентификационной и идентификационной информации;

использовать ставшие доступные ему, в ходе исполнения обязанностей, идентификационные данные пользователей для маскирования своих действий;

использовать в своих и (или) в чьих-либо личных интересах ИТ-ресурсы и предоставлять такую возможность другим;

передавать третьим лицам информацию ограниченного доступа (данные сетевой связанности, сетевые адреса, имена, пароли, информацию о привилегиях пользователей, настройки конфигураций средств и механизмов защиты информации и т.д.);

самостоятельно отключать средства и механизмы защиты информации, кроме случаев оговоренных настоящей Инструкцией и нормативными документами Госкорпорации «Росатом» и АО «Гринатом», а также при выводе их из эксплуатации;

производить действия, приводящие к нарушению порядка функционирования средств и механизмов защиты информации;

нарушать правила эксплуатации программных, аппаратно-программных средств и механизмов защиты информации.

корректировать, удалять, подменять информацию, содержащую регистрационные данные о событиях безопасности, журналы аудита.

самостоятельно (без согласования с администратором ИБ, выполняющим работы по контролю за соблюдением требований по безопасности информации) вносить изменения в состав и настройки СрЗИ, системного и прикладного ПО.

7 Специальные требования по ландшафтам информационной системы

Для установки ИС могут привлекаться работники соответствующих подразделений или обслуживающей организации, при этом администратор ИС обязан проверить корректность проведённой установки компонентов ИС.

Для разработки, тестирования и обеспечения защиты продуктивной системы от непроверенных или несогласованных изменений ИС имеет трехсистемный ландшафт, состоящий из продуктивного сегмента, тестового сегмента и сегмента разработки.

Продуктивный ландшафт, тестовый ландшафт и ландшафт разработки ИС размещается в соответствующем тенанте и плече ЗКО в соответствии с утвержденной документацией.

Работы по установке, конфигурированию ИС в тестовом и продуктивном ландшафте должны проводится при условии извещения о них АИБ СЦУДП в соответствии с разделом 8 настоящей инструкции.

Все настройки и разработки ПО ИС проводятся только в специальной зоне разработки тестового ландшафта и ландшафта разработки с использованием тестовых данных. Когда в процессе настройки и разработки достигается приемлемый уровень, при помощи транспортной системы осуществляется перенос изменений в систему контроля качества, которая служит для тестирования

изменений. По окончании тестирования настройки переносятся в эталонную систему.

В продуктивном ландшафте ИС запрещено выполнять действия, связанные с разработкой и отладкой компонентов ИС.

В тестовом ландшафте и ландшафте разработки запрещено обрабатывать конфиденциальную информация без наличия на них аттестата соответствия требованиям безопасности или положительного заключения проверки соответствия требованиям ИБ.

8 Порядок изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения

Все изменения условий эксплуатации, состава и конфигурации технических средств и ПО ИС должны производиться только на основании заявок руководителей структурных подразделений, согласованных установленным порядком с учётом требований, предъявляемых к аттестованным объектам информатизации.

Право внесения изменений в конфигурацию технических средств ИС предоставляется уполномоченным исполнителям в отношении изменения условий эксплуатации, состава и конфигурации технических средств и программного обеспечения – работникам соответствующих подразделений или обслуживающей организации.

Порядок изменения условий эксплуатации, состава и конфигурации технических средств и ПО:

начальник структурного подразделения оформляет заявку на внесение изменений;

АИБ СЦУДП подтверждает производственную необходимость проведения указанных в заявке изменений и отсутствие нарушений требований безопасности информации;

утверждённая заявка передаётся уполномоченному исполнителю для проведения работ по заявке;

руководитель подразделения допускает уполномоченных исполнителей для непосредственного исполнения работ при предъявлении утверждённой заявки;

если для проведения работ по утверждённой заявке необходимо внесение временных изменений в состав или настройки СрЗИ ИС, то данные работы проводятся уполномоченными исполнителями под контролем АИБ СЦУДП;

установка и обновление ПО производится администратором ИС с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком, или с эталонных копий программных средств;

по завершению выполнения работ по заявке, уполномоченные исполнители делают отметку о выполнении и передают исполненную заявку АИБ СЦУДП;

на основании исполненной заявки администратор вносит изменения в организационно-распорядительные документы на ИС.

При возникновении аварийных (нештатных) ситуаций для восстановления ИС необходимо руководствоваться принятым DRP планом по действиям в аварийных и нештатных ситуациях.

9 Порядок осуществления контроля функционирования информационной системы

Порядок осуществления администратором ИС контроля функционирования ИС СЦУДП в соответствии с документом «Программное средство «Система централизованного управления доступом пользователей» (СЦУДП) «Руководство администратора» (код документа 64509942.00214-01 96 01), раздел 3.8.3:

проведение регулярных РР (просмотр оперативных журналов, дампов и т.д.), направленных на своевременное выявление отклонений от нормального режима функционирования ИС СЦУДП и оперативного реагирования на подобные события.

Приложение

Лист ознакомления

№	ФИО	Должность	Дата	Подпись

Руководитель подразделения _____

Ф.И.О. подпись